# 一种改进的椭圆曲线密码实现算法

李　湛
（复旦大学数学系，上海　200433）

**摘　要**　椭圆曲线密码系统(ECC)与其他公钥体制相比，是迄今为止每比特具有最高安全强度的密码系统。椭圆曲线密码的算法研究的一个方向是进一步减少算法的运算量，以便于该算法在实际环境中应用。椭圆曲线上的倍点和数乘运算是椭圆曲线中核心运算，该文通过对计算过程的深入研究，推导了直接计算$2^m P, m \pm 1$的公式，并从理论上分析直接计算所节省的计算量。进而对椭圆曲线密码的快速实现算法进行了相应的改进，所提出的新算法的性能随着直接计算$2^m P, m \pm 1$中$m$的增大而提高，在极限情况下性能可比原算法提高30%，具有较大的应用价值。

**关键词**　椭圆曲线密码；算法实现；性能改进

**中图分类号**　TP309.2

## 1 引　言

随着信息技术和网络技术的不断发展和应用，电子信息的安全性问题变得越来越重要。而密码学作为信息安全的核心，在信息安全中扮演着极为重要的角色。信息安全使用的密码技术，基本上可分为：序列密码、对称密码（又称分组密码，如 DES，AES 等）和非对称密码（又称公钥密码，如 RSA，椭圆曲线算法—ECC 等）。RSA 是目前较为流行的公钥算法，但 ECC 相对于 RSA 有着许多让人无法抗拒的优越性。

椭圆曲线密码系统（ECC），即基于椭圆曲线离散对数问题的各种公钥密码体制，最早是在 1985 年分别由 V.S.Miller[1]和 Neal Koblitz[2]独立提出的。从 1985 年以来，ECC 受到了全世界密码学家、数学家和计算机科学家的密切关注。许多研究成果和应用实例不断涌现。

ECC 相对于 RSA 和 DSA 等系统在解决其数学问题椭圆曲线离散对数问题（ECDLP）时也要用完全指数时间。因此与 RSA 和 DSA 等系统相比，在同样安全强度下椭圆曲线密码系统具有计算量小，处理速度快，存储空间少，带宽要求低的优点。这使 ECC 在无线网络等受限环境中具有广阔的应用前景。

## 2 椭圆密码体制实现中的快速算法

由于加密、解密的设备一般都要受到计算速度和存储容量的限制，因此椭圆曲线密码体制的快速算法一直是椭圆曲线密码研究中的一个重要问题。

由文献[3]中的椭圆曲线密码的基础知识可知：在椭圆曲线中，当设$Q = nP, P, Q \in E(F)$时，从$n, P$求$Q$存在有效的算法，而从$P, Q$求$n$没有有效的算法，这个问题就称为椭圆曲线离散对数问题。正是基于这一特性，就可以仿照ElGamal类加密体制和签名方案，Diffie-Hellman密钥交换方案构造密码体制。

在椭圆曲线密码体制中，从$n, P$求$Q$，称为椭圆曲线中的数乘运算，它是密码体制实现中的核心步骤。目前从$n, P$求$Q$一般通用的算法是Binary Algorithm，k-ary Method，Sliding Window Method等。在这些算法中，从$P$计算$2^s P, s \pm 1$是核心步骤，一般而言，目前常用的算法中$s$取8。这种运算通常称为倍点运算，是椭圆曲线中一个核心运算，是数乘运算的基础，也是加密过程中最常用的运算。该文将要深入研究的就是加速倍点运算的方法。

## 3 已有的工作分析

根据椭圆曲线倍点公式[4]，设

$P = (x, y) \in E(F_{2^q}), 2P = (x_1, y_1)$，其中：

收稿日期：2004-05-02

$$x_1=\left(x+\frac{y}{x}\right)^2+(x+\frac{y}{x})+a,$$

$$y_1=x^2+(x+\frac{y}{x})x_1+x_1.$$

由于在计算过程中一般要用到$2^kP,k\geq 1$，可以一步一步地计算 $2P$, $2^2P$, $2^3P\cdots$，但这样效率较低。文献[4]中提到可以直接计算$4P,8P,16P$来计算$2^mP,m\geq 1$,而不是一步一步计算$2P, 2^2P, 2^3P\cdots$。

文献[4]中算出$4P=(x_2,y_2)$，其中

$$x_2=\frac{\zeta^2+(\delta\gamma)\zeta}{(\delta\gamma)^2}+a,y_2=\frac{\zeta(\delta\gamma)x_2+(\delta^2)^2}{(\delta\gamma)^2}+x_2$$

$$\gamma=x^2,\eta=\gamma+y,\delta=\eta^2+\eta x+a\gamma,$$

$$\xi=\eta x+\gamma,\zeta=\delta(\delta+\xi)+\gamma^2$$

从以上表达式中可以看到,虽然直接计算 $4P$ 与先算 $2P$ 再算 $2\cdot 2P$ 相比需要多计算 9 次乘法，但可以少计算一次求逆运算。由于 1 次求逆的时间通常多于 9 次乘法的时间,这样做就能有效地减少运算时间。

## 4 一种新的改进算法

在对以上方法研究的基础上可以将其进行推广,给出直接计算$2^sP,1\leq s\leq m$的公式,这样做可以进一步减少计算量。先推导出$2^sP,1\leq s\leq m$的表达式。记$2^kP=(x_k,y_k)$，则:

$$x_k=(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})^2+(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})+a,$$

$$y_{k-1}^2=x_{k-1}^2+(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})x_k+x_k$$

这里要做的是把$(x_k,y_k)$直接表示成$x_k=\frac{a_k}{c_k}+a,y_k=\frac{b_k}{c_k}$的形式。其中,$a_k,b_k,c_k$都是关于$x,y$的整式,这样就实现了用乘法来减少求逆的目的。将$x_k=\frac{a_k}{c_k}+a,y_k=\frac{b_k}{c_k}+x_k$代入递推式,就得到了$a_k,b_k,c_k$的递推式如下:

$$c_k=\delta^2,a_k=\gamma^2+\delta\gamma,b_k={a_{k-1}}^4+\delta\gamma x_k$$

其中 $\delta=a_{k-1}c_{k-1},\gamma={a_{k-1}}^2+b_{k-1}c_{k-1}$，而

$a_0=x,b_0=y,c_0=1$。

由此递推公式，来估计用改进过的方法的计算量。在改进的方法中计算$2^sP,1\leq s\leq m$的运算量为 $4s$ 次乘法，$4s$ 次平方，1 次求逆，而逐次计算$2^sP,1\leq s\leq m$则需要 $2s$ 次乘法，$2s$ 次乘方，$s$ 次求逆。总的运算量可通过表 1 进行比较，其中加法计算次数由于直接计算和逐次计算相差不大,故忽略。

表 1　不同方法运输量的比较

| 计算的值 | 计算方法 | 乘法 | 平方 | 求逆 | 总时间(μs) | 节省率 |
|---|---|---|---|---|---|---|
| $4P$ | 直接计算 | 8 | 8 | 1 | 501.05 | |
| | 逐次计算 | 4 | 4 | 2 | 488.62 | |
| $8P$ | 直接计算 | 12 | 12 | 1 | 710.77 | 1.3% |
| | 逐次计算 | 6 | 6 | 3 | 720.24 | |
| $16P$ | 直接计算 | 16 | 16 | 1 | 920.49 | 5.8% |
| | 逐次计算 | 8 | 8 | 4 | 977.24 | |
| $2^sP(s\to\infty)$ | 直接计算 | $4s$ | $4s$ | 1 | $169.16s+158.73$ | 30.5% |
| | 逐次计算 | $2s$ | $2s$ | $s$ | 243.31s | |

表 1 中总时间由表 2 算出，见文献[4]。

表2 计算时间比较

| 操作类型 | 计算时间比较（总时间/μs） |
|---|---|
| 176 bit addition | 1.19 |
| 176 bit squring | 4.23 |
| 176 · 176 bit multiplication | 38.56 |
| 176bit inverse | 158.73 |

## 5 结 论

从文中可以看出，通过直接计算$2^s P, 1 \leqslant s$而非间接计算$2^s P, 1 \leqslant s$，本质上将费时的域中求逆元算替换成了较快的平方或乘法等运算，因此减少了计算量，加快了运算速度。从以上结果可以看出，笔者提出的新算法的性能随着直接计算$2^m P, m \neq 1$中$m$的增大而提高，在极限情况下性能可比原算法提高30%，因此有较大的应用价值。

## 参考文献


1 Miller V. Use of Elliptic Curves in Cryptography. In Cryptology Springer-Verlag, 1986, 417~426.

2 Koblitz N. Elliptic Curve Crystosyestems. Mathematics of computation, 1987,48(177):203-209.

3 Blake I.F, Seroussi G, Smart N.P, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

4 Guajardjo J, Paar C, Efficient algorithms for elliptic curve cryptosystems. Advances in Cryptology, Proceedings ofEurocrypt'97. Springer-Verlag, 1997, 342~356.



**作者简介**

**李湛，男，复旦大学数学系。**


# An Improved Implementation Method on Elliptic Curve Cryptography


Li Zhan

(Department of Mathematics, FuDan University, Shanghai 200433, China)



**Abstract** Compared with previous public key schemes, this improved Elliptic Curve Cryptography has the highest secure strength-per-bit. One of the major research fields of the Elliptic Curve Cryptography is to reduce its complexity so as to be conveniently applied. Since multiplication of points and scalar multiplication of points are key operations in elliptic curve cryptography, this paper deduces through in-depth researches into the calculating process a formula to calculate $2^m$P, m≥1 directly and analyzes in theory the amount of operation saved by using this method. Furthermore, the new algorithm for calculating $2^m$P, m≥1 directly can effectively improve the calculating performance with the increase of $m$. Therefore, the performance of the new algorithm can be improved by 30% at most to the original one, thus making it a desirable algorithm of great value.



**Keyword** Elliptic Curve Cryptography; algorithm implementation; performance improved